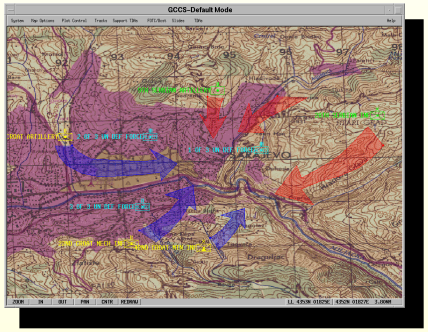
Defense Information Systems Agency (DISA) Securing Computing

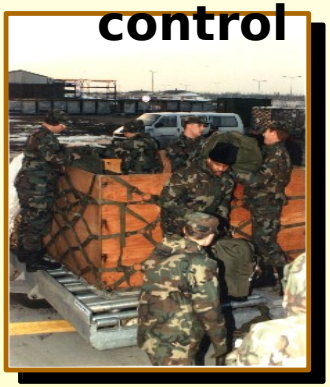
Mr. David Hughes
14 January 2003
(717) 267-9901
hughesd@ritchie.disa.mil

DISA Computing Services – Combat Support Processing

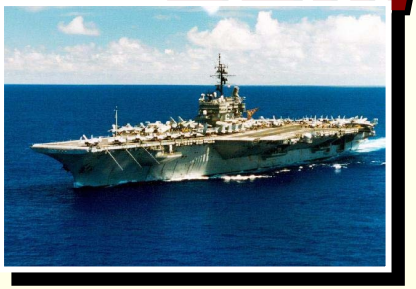
DISA runs the IT systems that -



provide command and control



manage parts and replenish supplies



provision ships

manage transportation

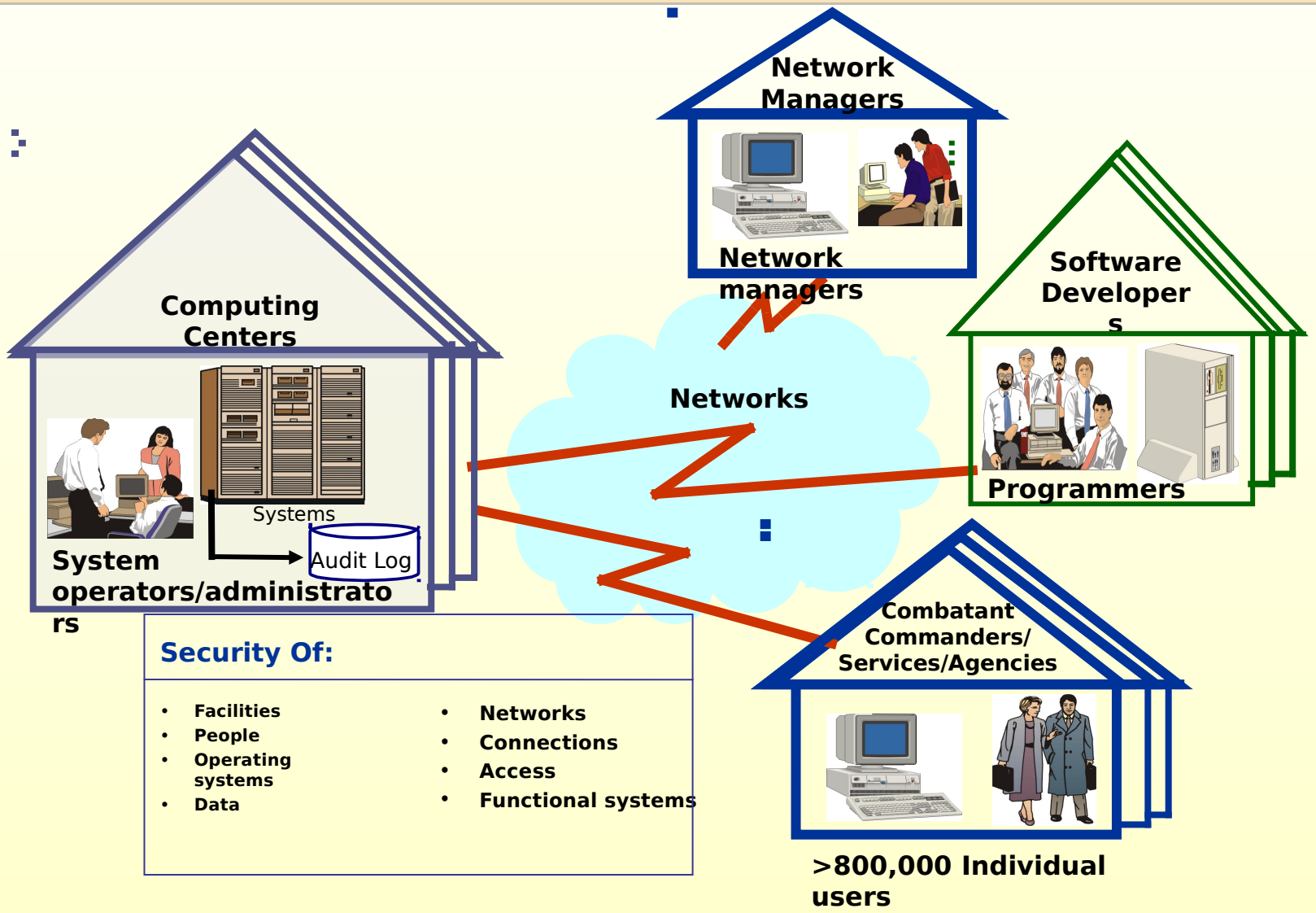
pay the warfighters

provide medical care

manage maintenance

Defense Data Centers

Scope of Security



Security Of:

- Facilities
- People
- Operating systems
- Data
- Networks
- Connections
- Access
- Functional systems

Information Assurance

Traditional security

- Clearance and background investigation required
- ADP position designation – ADP I or II
- Photo badges
- Access list/visitor control
- Access control to facility
- True wall computer room
- 24x7 operations
- Alarms
- Closed circuit TV
- Property control

Electronic security

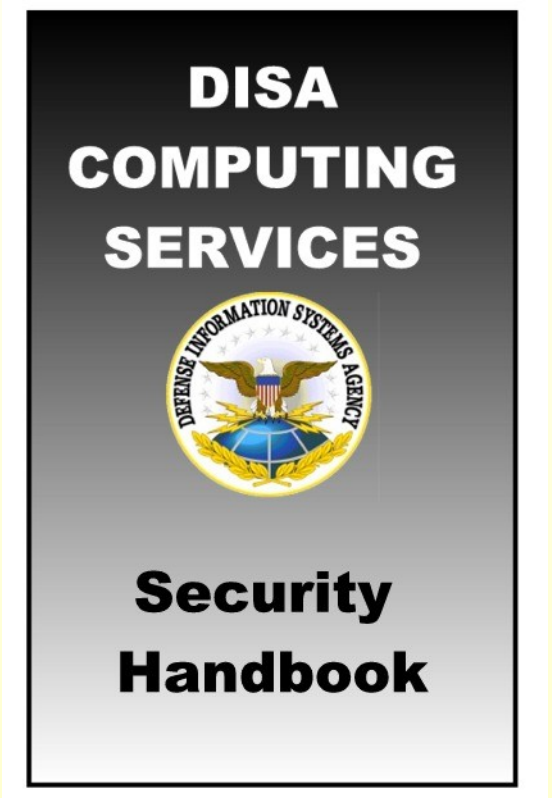
- Security Technical Implementation Guides (STIGs)
- Self assessment tools
- External security assessments
- Vulnerability management system
- Employee training/certification
- Security accreditation program
- Network and host intrusion detection
- Router access control
- Firewalls
- Audit servers
- Automated policy enforcement
- Virus protection
- Demilitarized zones

Traditional Security

DISA's Security Handbook

Addresses each of these topics:

- **Personnel security**
- **Information security**
- **Physical security**
- **Industrial security**
- **Information systems security**
- **Communications security**
- **Emanations security**
- **Operations security**



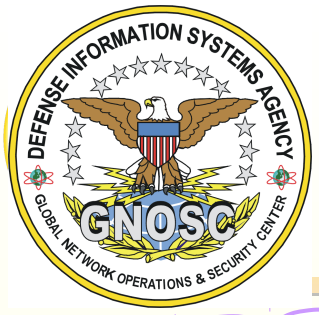
Traditional Security Highlights

- Data centers located on military base or federal facility with controlled entry
- Controlled access to data centers
  - Secondary controls at computer room
  - Computer rooms alarmed with 24 hour police response
- Closed circuit TV monitoring 24x7
- Background investigation required for all employees
- All personnel require badges
  - Differentiate among federal and contractor employees and personnel requiring escort
  - Access lists are maintained
  - Visitors must sign in
- Property control, including inventory and bar codes

Electronic Security

- **Security Technical Implementation Guide (STIG): A guide for information security**
- **A compendium of security regulations and best practices from many sources that apply to an operating system or a part of the Defense infrastructure**
- **Goals**
  - **Intrusion avoidance**
  - **Intrusion detection**
  - **Response and recovery**
  - **Security implementation guidance**
- **Checklists and evaluation scripts provided for each technology**

Defense-in-Depth



GIG
Connectivity

RCERT

Global Network IDS

Virus Protection

Communities of Interest

Host IDS

Host IDS

Vulnerability Assessment

Firewalls

Premise Routers

Local Network IDS

Electronic Switches

DMZ

Public Web Servers
EC/EDI

System Mgt Center

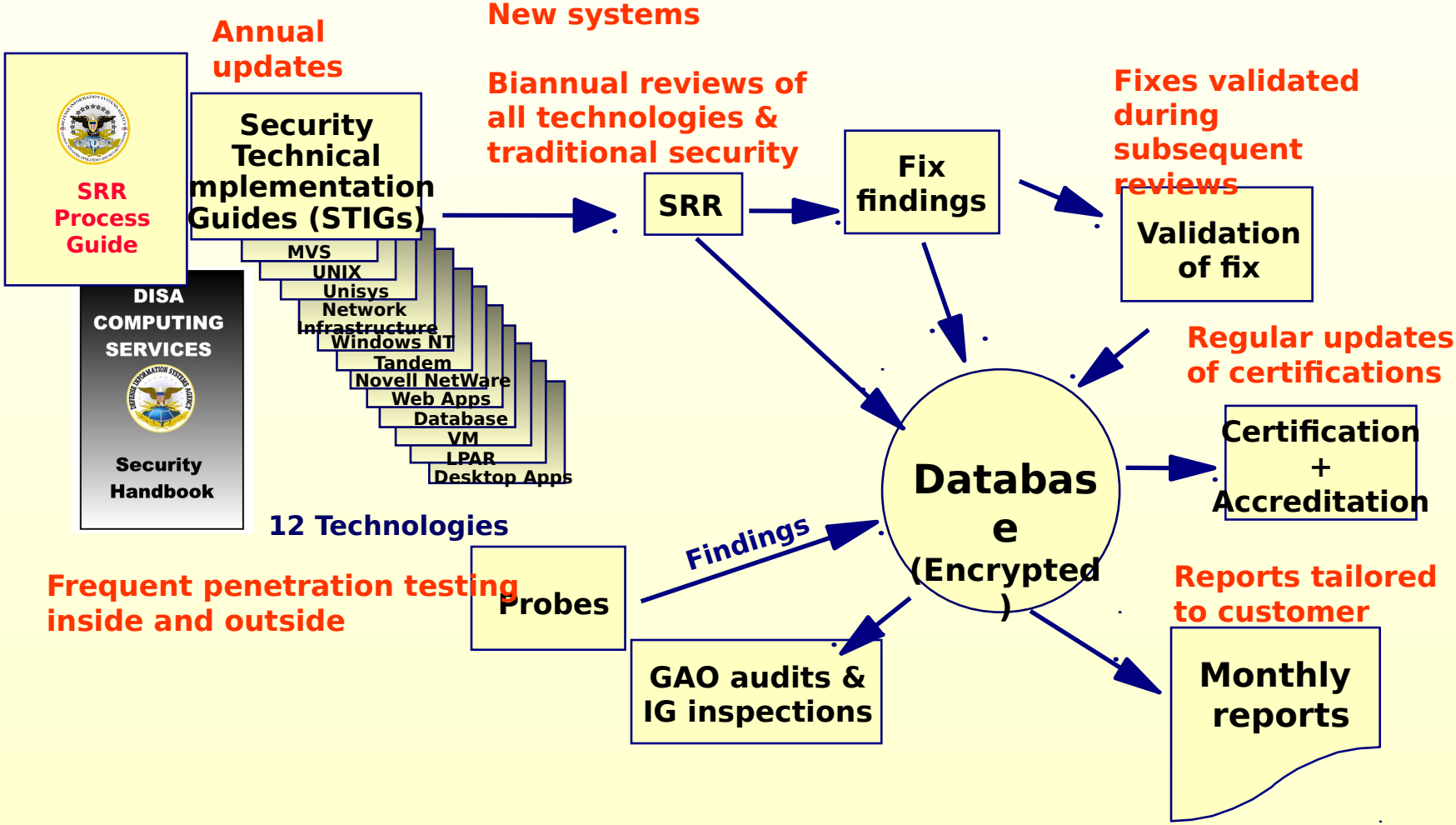
IA Tool Master Consoles

Audit Server

Electronic Security Highlights

- Robust technical security standards
- Tools, checklists, scripts for self-assessment
- Annual independent reviews to ensure standards enforcement
- Vulnerability Management System (VMS)
  - All findings tracked to resolution
  - Registrations of all assets
  - Identification of new vulnerabilities
- Training and certification programs
- Two levels of intrusion detection

DISA Security Readiness Review (SRR) Process



"A fanatic is someone who can't change his mind and won't change the subject."

Sir Winston Churchill

Computer Network Defense Information Assurance

"We need to be fanatics . . . about National Security"

and . . .

PROTECT AND DEFEND THE DEFENSE INFORMATION INFRASTRUCTURE (DII)

DEFENSE INFORMATION SYSTEMS AGENCY